Jason "Jay" Barnes (*pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (*pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (*pro hac vice*)
atruong@simmonsfirm.com
Sona R. Shah (*pro hac vice*)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: 212.784.6400
Facsimile: 212.213.5949

Christian Levis (*pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (*pro hac vice*)
afiorilla@lowey.com
Rachel Kesten (*pro hac vice*)
rkesten@lowey.com
Yuanchen Lu (*pro hac vice*)
ylu@lowey.com
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: 914.997.0500
Facsimile: 914.997.0035

Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice*)
lpittman@lchb.com
Danna Elmasry (*pro hac vice*)
delmasry@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Facsimile: 415.956.1008

Philip L. Fraietta (SBN 354768)
pfraietta@bursor.com
Max S. Roberts (*pro hac vice*)
mroberts@bursor.com
Victoria X. Zhou (*pro hac vice*)
vzhou@bursor.com
Joshua R. Wilner (SBN 353949)
jwilner@bursor.com
BURSOR & FISHER, P.A.
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: 914.874.0710
Facsimile: 914.206.3656

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE THE TRADE DESK, INC. DATA PRIVACY LITIGATION

Case No. 3:25-cv-2889 (CRB)

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Judge: Hon. Charles R. Breyer
DATE: December 19, 2025
TIME: 10:00 a.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

Statutes

TABLE OF AUTHORITIES
(continued)

Page

I. SUMMARY OF ARGUMENT

The Trade Desk, Inc. ("TTD") conducts surreptitious mass-surveillance of Americans through the collection and aggregation of personal data, analyzing that data to create comprehensive "cradle-to-grave" dossiers, with thousands of data points concerning the location, activities, and preferences of millions of individuals with whom it has no direct relationship. TTD sells products and services generated from these dossiers to its customers, who use it to influence the commercial, social, and political behaviors of Americans without their knowledge or consent. TTD's conduct goes far beyond any reasonable notion of "routine commercial behavior." These practices involve persistent, real-time tracking and the construction of detailed, individualized profiles that monitor the most intimate aspects of people's lives, which can be used to further surveil, target, and manipulate them.

TTD's conduct offends established legal protections of privacy.

Article I, Section 1 of the California Constitution and longstanding common law enshrine privacy as an inalienable right. Recent jurisprudence within this Circuit and District holds that the aggregation of large quantities of data can itself violate reasonable expectations of privacy, even if individual data points are not sensitive in isolation, especially when they are subject to algorithmic computer intelligence to yield inferred, sensitive personal data which are centralized in individualized dossiers containing intimate details of people's personal lives. *See In re Facebook, Inc. Internet Tracking Litig*. ("*Facebook Tracking*"), 956 F.3d 589, 601–04 (9th Cir. 2020); *Katz-Lacabe v. Oracle Am., Inc*., 668 F. Supp. 3d 928, 942 (N.D. Cal. 2023); *Riganian, et al. v. LiveRamp Holdings, Inc*., 2025 WL 2021802, at *7–8 (N.D. Cal. July 18, 2025). Contrary to TTD's assertions, the California Consumer Privacy Act ("CCPA") as amended by the California Privacy Rights Act ("CPRA") was enacted to supplement—not supplant—privacy protections, and thus provides no basis to dismiss any claim.

TTD's real-time interception of the contents of electronic communications and the collection of electronic addressing information fall squarely within the scope of the California Invasion of Privacy Act ("CIPA") and the federal Electronic Communications Privacy Act ("ECPA"). *See Riganian*, 2025 WL 2021802, at *10-11; *Brown v. Google LLC*, 685 F. Supp. 3d

909, 939 (N.D. Cal. 2023); *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *2–4 (N.D. Cal. June 9, 2023). TTD's arguments regarding consent, "in transit" interception, and the rule of lenity are contrary to law and raise factual issues not resolvable on this motion. TTD's narrow interpretation of the pen register provision is foreclosed by the statutory text and the broad remedial purpose of the law, as recognized by every federal court to consider the issue, including this Court. *See Mirmalek v. Los Angeles Times Commc'ns LLC*, 2024 WL 5102709, at *3–4 (N.D. Cal. Dec. 12, 2024) (Breyer, J.); *Fregosa v. Mashable, Inc.*, 2025 WL 2886399, at *9 (N.D. Cal. Oct. 9, 2025) (Breyer, J.).

Plaintiffs' allegations that TTD's technology violates the California Comprehensive Data Access and Fraud Act ("CDAFA") by causing the unauthorized access, loss, and the introduction of computer contaminants is precisely the type of conduct CDAFA outlaws. *Smith v. Rack Room Shoes, Inc.*, 2025 WL 2210002, at *3 (N.D. Cal. Aug. 4, 2025); *Rodriguez v. Google LLC*, 772 F. Supp. 3d 1093, 1110 (N.D. Cal. 2025). TTD is simply wrong that CDAFA only prevents "computer hacking" and that Plaintiffs cannot show "tangible harm."

Finally, California law recognizes a right to unjust enrichment where, like here, an entity unjustly benefits from the misappropriation and use of data. This form of equitable relief is legally appropriate because TTD wrongfully profits at the expense of Plaintiffs' privacy rights, and privity is not required for such a claim under California law. *See Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 6466195 at *6 (N.D. Cal. Oct. 3, 2023); *Riganian*, 2025 WL 2021802 at *12–13. For these reasons, and as set forth below, TTD's motion to dismiss should be denied in its entirety.

II. INTRODUCTION

Plaintiff class representatives are concerned and injured citizens who allege that Trade Desk's invasive and surreptitious digital surveillance practices are egregious and serious invasions of privacy interests long recognized in our society and well-established law. TTD assigns individuals a unique, persistent identifier, effectively its home grown version of a new social security number, using it to track individuals as it aggregates vast quantities of their online *and offline* personal data gathered across websites, devices, and real-world locations and activities. It combines and analyzes this data to create detailed "cradle-to-grave" dossiers on Plaintiffs and Class

members. TTD's dossiers encompass sensitive behavioral, demographic, and transactional information, enabling TTD to make inferences about the most intimate aspects of individuals' lives. Contrary to TTD's rhetoric, nothing about this case challenges the online advertising industry as a whole, but rather targets TTD's (and *only* TTD's) uniquely invasive conduct—conduct that far exceeds the bounds of routine commercial activity in ways that violate the law.

TTD's scattershot motion resorts to a radical and unsupported declaration that the CCPA and CPRA entirely supplanted all existing privacy protections in the electronic sphere. This direct attack on the foundational principles of California privacy law is flatly contradicted by the language of the CCPA and CPRA, and has accordingly been rejected by every court to have considered it. TTD's argument would, in essence, have this Court hold that decades of California and federal privacy jurisprudence—including recent jury verdicts and appellate decisions—were wrongly decided, and that the conduct found illegal by juries in cases like *Frasco v. Flo Health, Inc.*,[1] and *Rodriguez v. Google LLC*,[2] is not only legal, but affirmatively protected. That is not the law.

Plaintiffs' invasion of privacy claims challenge not just TTD's collection of their "internet activity," but its surreptitious creation of comprehensive profiles on millions of individuals by aggregating vast quantities of online *and offline* data—including tens of thousands of data points collected from data brokers and other third parties such as financial reporting, health and medical data providers, retailers, and even from Class members' bedrooms through their home devices like internet-connected TVs. TTD's motion willfully ignores these core allegations and the overwhelming weight of authority holding that such comprehensive and invasive profiling by commercial actors violates fundamental privacy rights.

TTD's Wiretap Act, CIPA, and CDAFA defenses are similarly infirm: the complaint plausibly alleges contemporaneous interception of communication contents, defeating TTD's "in transit" and "no contents" arguments, TTD's cramped reading of California's pen-register statute

[1] No. 3:21-cv-00757 (N.D. Cal. Aug. 1, 2025) (jury verdict against Meta for violation of CIPA § 632 where Meta's analytics technology collected users' information entered into the Flo fertility-tracking app).

[2] No. 5:20-cv-04688 (N.D. Cal. Sept. 3, 2025) (jury verdict for plaintiffs on constitutional and common law privacy claims arising from Google's collection of data through its analytics software).

contradicts the text and remedial purpose, and its lenity argument has been repeatedly rejected by every federal court to consider the issue, including this Court. CDAFA is satisfied by well-pleaded allegations of access "without permission," introduction of computer contaminants, and cognizable loss including loss of control over data and depletion of device resources, which courts in this District have recognized as sufficient. Likewise, TTD's perfunctory challenge to unjust enrichment is foreclosed by recent, directly on-point authority finding the claim applicable in identical circumstances. The motion to dismiss should therefore be denied in full.

III. FACTUAL BACKGROUND

A. Trade Desk's Conduct

This case challenges TTD's unlawful surveillance and profiling of millions of people. Consolidated Class Action Complaint, Dkt. No. 52 ("CCAC") ¶¶ 2, 68. TTD has no first party relationship with the individuals it surveils—no contract and no exchange of promises or services—which means class members are unlikely to even know of TTD's *existence*, and are unable to have consented to its conduct. TTD's profiles are anchored by its bespoke identifier known as "Unified ID 2.0" ("UID2")—the equivalent of a universal "online social security number"—that TTD uses to permanently link data collected about a person's online and offline activities to that specific individual. *Id*. ¶¶ 68, 75–81. This allows TTD to create comprehensive "cradle-to-grave" dossiers that encompass, beyond basic identifying information, a vast array of sensitive and intimate details, including web browsing histories, real-world purchases, geolocation data, health conditions, political views, financial status, and more, that are subject to algorithmic computer intelligence to yield further inferred, sensitive personal information. *Id.* ¶¶ 8–53, 115–123. TTD's tracking technologies—deployed across hundreds of thousands of websites—continuously update and refine these profiles, which TTD sells to advertisers and data brokers through its "Data Marketplace," and who can subsequently use that data to further surveil and manipulate people. *Id.* ¶¶ 1, 87–114. Critically, TTD's motion ignores Plaintiffs' allegations that TTD combines this "online" data with extensive *offline* data collected from third parties, which it uses to build profiles on Plaintiffs consisting of *tens of thousands* of data points. *Id.* ¶¶ 12–38.

TTD has been described as a "giant[] in online advertising," on par with serial privacy

violator Google. *Id.* ¶ 66. TTD is a central node in the real-time bidding ("RTB") ecosystem, where it receives, processes, and transmits bids for digital ad space. *Id.* ¶¶ 69–72, 108–113. TTD discloses granular information—such as device identifiers, IP addresses, geolocation, browsing activity, and other personal attributes (*Id.* ¶¶ 65–72, 108–14)—in response to each bid, as advertisers determine what (and if) they are willing to pay to display an ad to the particular individual. *Id.* TTD leverages its UID2 infrastructure to match and enrich these "bidstream" data with its own persistent profiles, enabling advertisers to target individuals with extraordinary precision across websites, devices, and contexts. *Id.* ¶¶ 65–72, 108–45. This integration of persistent "identity resolution"[3] with the RTB infrastructure enables TTD to maintain and monetize highly detailed profiles on millions of individuals, amplifying the scope and impact of its invasive surveillance far beyond traditional advertising practices. *Id*.

B. The Representative Plaintiffs

The experiences of the four named Plaintiffs illustrate the real-world consequences of TTD's surveillance practices. Each Plaintiff discovered, through TTD's responses to statutorily-mandated data-access requests, that TTD had assigned to them persistent UID2 identifiers, collected extensive information regarding their devices, precise geolocation, and extensive browsing histories, and constructed vast, persistent profiles on them—containing tens of thousands of data points drawn from multifarious third parties and data brokers, that revealed not only their browsing habits, but also deeply personal and sensitive information such as health conditions, political beliefs, financial status, and even inferred emotional states. CCAC ¶¶ 5–53.

For example, among the 32,340 unique advertising "segments," or categories, associated with Plaintiff Michie, TTD compiled and offered for sale detailed information reflecting his voting history and political views on issues such as abortion, gun control, and immigration; his physical and mental health conditions, insurance, and medication use; his income, mortgage, credit, and spending patterns; and his personal shopping, travel, and media consumption habits. *Id.* ¶ 12. TTD similarly profiled and sold information about Plaintiff Justin Dyer's political view and financial

[3] "'Identity resolution' refers to the process of merging or resolving various distinct data points or touchpoints (an email address and a mobile device ID (or 'MAID'), for example) into a comprehensive identity profile of a single person." CCAC ¶ 76.

condition, *id.* ¶ 24, while Plaintiff Jessica Ju's dossier catalogued her health interests, political views, and precise geolocation, *id.* ¶¶ 37–38.[4] These detailed dossiers allow advertisers, including political campaigns, to target and manipulate Plaintiffs with incredible precision. TTD's motion utterly ignores the existence of this concrete, direct evidence of extensive dossier-building. None of the Plaintiffs ever consented to the creation or use of these detailed profiles in any form. *Id.* ¶¶ 5–53, 153–69.

IV. ARGUMENT

A. Plaintiffs' Invasion of Privacy Claims Stand

TTD willfully miscasts Plaintiffs' allegations of TTD's surveillance as about little more than vague and anodyne "internet tracking." TTD's diversion ignores the established jurisprudence in this Circuit and District, developed both before and after the enactment of the CCPA and CPRA, which confirms the rule that the aggregation of large quantities of data into individualized dossiers violates an objectively reasonable expectation of privacy, because regardless of the sensitivity of any of its component individual data points, the aggregation of that data permits highly intrusive and reliable inferences and predictions of character and behavior, which *are* revealing of sensitive, private matters. *See Facebook Tracking*, 956 F.3d at 601-04; *Katz-Lacabe*, 668 F. Supp. 3d at 942; *Katz-Lacabe*, 2023 WL 6466195 at * 9 (N.D. Cal. Oct. 3, 2023) (subject data "indicate[s] more than simple likes or dislikes and instead communicate[s] intimate details of Plaintiffs' daily lives"); *Riganian*, 2025 WL 2021802, at *6–7; *Brooks v. Thomson Reuters,* 2021 WL 3621837, at *9 (N.D. Cal. Aug. 16, 2021). Indeed, in 1972 the People of California amended the California Constitution to address the highly offensive emergence of "cradle-to-grave" digital dossiers—precisely the conduct challenged here. *See* Ballot Pamp., Proposed Stats. & Amends. to Cal. Const. With Arguments to Voters. Gen. Election *26 (Nov. 7, 1972).

A claim for intrusion upon seclusion under California common law requires (1) intrusion into a private place, conversation, or matter to which Plaintiffs have a reasonable expectation of privacy (2) "in a manner highly offensive to a reasonable person." *Facebook Tracking*, 956 F.3d at

[4] Plaintiff Turner also requested her data from TTD but TTD did not provide it as of the filing of the Consolidated Class Action Complaint. *See* CCAC ¶ 45.

601. To state a claim for invasion of privacy under the California Constitution, Plaintiffs must show "(1) a legally protected privacy interest, (2) a reasonable expectation for privacy, and (3) the intrusion is so serious as to amount to an egregious breach of social norms." *Id*. Given the similarity of the two tests, courts consider them together and ask whether (1) there is a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1088 (N.D. Cal. 2022). Plaintiffs have adequately alleged both claims.

1. Plaintiffs Have Alleged a Reasonable Expectation of Privacy

Controlling precedent establishes that Plaintiffs have adequately alleged a reasonable expectation of privacy that is intruded upon by the systematic collection of data of the details of their daily lives. In *Facebook Tracking*, plaintiffs alleged that Facebook obtained "an enormous amount of individualized data" by collecting URLs of third-party websites that could potentially "divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's platform," thereby gaining "cradle-to-grave profile[s]" of internet users without their consent. 956 F.3d at 603, 605. Facebook's alleged compiling of "highly personalized profiles from sensitive browsing histories and habits" prevented any conclusion that the plaintiffs failed to allege a reasonable expectation of privacy. *Id.* at 604 n.7 (citing *Carpenter v. U.S.*, 138 S. Ct. 2206, 2217 (2018); *Riley v. California*, 573 U.S. 373, 397–99 (2014)). The Ninth Circuit emphasized that "individuals have a reasonable expectation of privacy in collections of information that reveal 'familiar, political, professional, religious, and sexual association'" and that "individuals maintain the expectation that entities will not be able to collect such broad swaths of personal information absent consent." *Id.* at 604 n.7.

District courts have since consistently applied *Facebook Tracking* to find reasonable expectations of privacy in aggregated data. In *Katz-Lacabe v. Oracle*, the court confronted allegations that ad tech giant Oracle invaded plaintiffs' privacy through its "ID Graph" identity resolution services and Data Marketplace—both functionally identical to the UID2 and Data Marketplace services offered by TTD. In rejecting the same argument that TTD makes here, that "the data allegedly collected was not sensitive [or private] in nature" and that plaintiffs had no expectation of privacy in their internet activity, the court stated: "Plaintiffs' strongest argument lies

in its allegation that Oracle's accumulation of a 'vast repository of personal data'—from compiling Plaintiffs' browsing activity, online communications, *and* offline activity—is what contravenes the reasonable expectation of privacy. This is in line with the analysis provided in *Facebook Tracking*." *Katz-Lacabe*, 668 F. Supp. 3d at 942 (emphasis in original). In *Riganian v. LiveRamp*—involving allegations saliently identical to those both here and in *Katz-Lacabe*—the court found a reasonable expectation of privacy "in the information that LiveRamp compiled across hundreds to thousands of disparate online and offline sources and then sold to third parties without their knowledge or consent." 2025 WL 2021802, at *6. The *Riganian* court agreed with the *Katz-Lacabe* court that "tracking and identity resolution to create persistent identifiers linked to comprehensive behavioral profiles, and a data marketplace enabling the sale of sensitive personal information" invades the reasonable expectation of privacy. *Id.* at 7. In *Fed. Trade Comm'n v. Kochava, Inc*, the court found, relying on *Facebook Tracking*, that allegations that Kochava "sells 'data designed to give its customers a '360-degree perspective' on the unique traits of millions of individual device users," stated an "invasion of privacy—which is substantial both in quantity and quality." 715 F. Supp. 3d 1319, 1325 (D. Idaho 2024). Similarly, in *Brooks v. Thomson Reuters Corp.*, involving a defendant compiling invasive cradle-to-grave profiles from disparate sources, the court held that "compiling bits of Plaintiffs' personal information scattered throughout the internet (and allegedly in non-public sources) into a dossier is a significant invasion of privacy," noting "[t]he Supreme Court has held that compiling disparate pieces of information about a person into a single dossier, even if the individual pieces of information are publicly available, constitutes a significant invasion of privacy." 2021 WL 3621837, at *9 (citing *U.S Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989)).

TTD ignores this authority even though its conduct is functionally indistinguishable. The Complaint alleges that TTD systematically collects, aggregates, and links vast quantities of data—including web browsing histories, real-world purchases, geolocation data, health conditions, political views, financial status, and more—all anchored to its own homemade persistent identifiers, such as UID2, that it assigns to nearly every individuals, all permitting the creation of individual "cradle-to-grave" profiles and inferences about Plaintiffs' political views, health conditions, sexual

preferences, and other personal characteristics. CCAC ¶¶ 2, 5–53, 115-123; *see also* 105 Ops. Cal. Att'y Gen. 26 (2022), 2022 WL 815641, at *2 (inferences drawn from personal information themselves constitute protectable personal information). Plaintiffs here allege the same type of panoptic aggregation and commercialization of personal information that these courts have found to adequately allege a violation of the reasonable expectation of privacy.[5]

TTD mischaracterizes these allegations in its attempt to analogize the Complaint to cases such as *Thomas v. Papa Johns Int'l, Inc*., and *Hubbard v. Google LLC*, which involved either the collection of limited, non-sensitive data on a single website or platform, or circumstances where the defendant's conduct was fully disclosed.[6] Courts have repeatedly distinguished these cases from those, like here, involving unknown third-parties that aggregate massive amounts of data from both online and offline sources. *See Katz-Lacabe*, 668 F. Supp. 3d at 942 (distinguishing "routine commercial behavior" from the "accumulation of a 'vast repository of personal data'"); *Riganian*, 2025 WL 2021802, at *6–7 (finding a reasonable expectation of privacy where the conduct involves persistent, surreptitious aggregation and identity resolution). As *Katz-Lacabe* explained, such allegations "go well beyond" "routine commercial behavior."[7] 668 F. Supp. 3d at 942.

---

[5] TTD's footnoted waving away of any reasonable expectation of privacy in the *tens of thousands of detailed and sensitive data points* collected on Plaintiffs in the Data Marketplace (Mot. at 8, fn. 6) directly contravenes this authority. *See* CCAC ¶¶ 12–38. TTD's insistence that Plaintiffs have not sufficiently alleged what sensitive information TTD has collected on them is directly refuted by Plaintiffs' extensive allegations on precisely those topics. *Id*. TTD's authorities are distinguishable on that basis. *See Virgil v. Time, Inc*., 527 F.2d 1122, 1126 (9th Cir. 1975) (publication of facts already made public by the plaintiff); *B.K. v. Eisenhower Med. Ctr*., 721 F. Supp. 3d 1056, 1064 (C.D. Cal. 2024) (failure to allege with specificity what information was disclosed or when).

[6] These cases do not categorically foreclose the possibility of a reasonable expectation of privacy with respect to a person's internet activity, as TTD suggests. *Thomas v. Papa Johns Int'l, Inc.*, 2024 WL 2060140, at *2 (S.D. Cal. May 8, 2024), *aff'd*, 2025 WL 1704437 (9th Cir. June 18, 2025) ("[t]his is not to say there can never be a reasonable expectation of privacy over internet activity"); *Hubbard v. Google* LLC, 2024 WL 3302066, at *7 (N.D. Cal. July 1, 2024) (distinguishing *Facebook Tracking* and similar cases because *Hubbard* did not involve "secret or deceptive data collection"). Here, Plaintiffs allege that TTD's data collection is on a vast scale, surreptitious, and without consumer knowledge or consent. CCAC ¶¶ 65–112, 153–69.

[7] TTD's citations are readily distinguishable on this basis. *See Gutierrez v. Converse Inc.*, 2023 WL 8939221, at *4 (C.D. Cal. Oct. 27, 2023) (chat sessions with a single website); *Jones v. Peloton Interactive, Inc.*, 720 F. Supp. 3d 940, 951 (S.D. Cal. 2024) (same); *Saeedy v. Microsoft Corp*., 2023 WL 8828852, at *4 (W.D. Wash. Dec. 21, 2023) (data collected by a single browser); *Saleh v. Nike, Inc*., 562 F. Supp. 3d 503, 524–25 (C.D. Cal. 2021) (data collected limited to Nike website); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1016–17 (N.D. Cal. 2012) (disclosure of users' profile viewing activity to other LinkedIn users where users expected their activity to be visible to other users).

Courts have also repeatedly rejected TTD's argument that a reasonable expectation of privacy only exists against a defendant who affirmatively represented it would not track users' activity—an argument that seeks to transmute the inalienable right to privacy into a creature of contract, bequeathed only at the pleasure of a corporate defendant that deigns it useful to make such representations. The court in *Riganian*, directly rejecting this argument, found that "while the Ninth Circuit in *Facebook Tracking* found relevant to its analysis that Facebook had represented that it would not collect information on users when they were logged out but did so nonetheless, it did not hold that such misrepresentations are required to establish a reasonable expectation of privacy." 2025 WL 2021802, at *6; *see also Katz-Lacabe*, 668 F. Supp. 3d 928 (reasonable expectation of privacy against party plaintiffs were not in privity with); *Griffith v. TikTok, Inc.*, 697 F. Supp. 3d 963, 971 (C.D. Cal. 2023) (rejecting same argument).

Against this backdrop, Trade Desk fundamentally misconstrues both the purpose and effect of the CCPA and CPRA and the controlling legal standards governing privacy expectations under California law. The CCPA and CPRA were enacted to supplement, not supplant, the longstanding constitutional and common law protections for privacy. TTD's quasi-preemption argument—that the CCPA and CPRA reflect voter acknowledgement and approval of its invasive surveillance, thereby eviscerating any expectation of privacy with respect to that conduct—turns the statutes' text and purpose on their heads. To the contrary, the CPRA expressly *condemns* the very conduct at issue here, noting that "some advertising businesses today use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests." Cal. Prop. 24 (2020) § 2(I). The CPRA further states that "consumers should have the information and tools necessary to limit the use of their information to *noninvasive proprivacy* advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of[.]" *Id.* (emphasis added). Far from blessing TTD's invasive, anti-privacy conduct, the CCPA and CPRA condemn it.

Moreover, the CCPA unambiguously states that it is "intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information," and that "law relating to consumers' personal information should be construed to harmonize with the

provisions of this title," but "in the event of a conflict between other laws and the provisions of this title, *the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control*." Cal. Civ. Code § 1798.175 (emphasis added). Every court to have considered some version of the argument that TTD advances has rejected it, finding it "meritless." *Brooks*, 2021 WL 3621837, at *6 (rejecting as "meritless" defendants' argument that conduct could not be "unfair" under the UCL because it was "expressly permitted by" the CCPA); *Kellman v. Spokeo, Inc*., 599 F. Supp. 3d 877, 897 (N.D. Cal. 2022) (rejecting defendant's argument that it could not be liable under California's UCL because the CCPA contained an "expressed exemption" for its conduct, finding the CCPA does not "expressly or impliedly set aside privacy-based tort claims"). Indeed, this Court, in *Mirmalek*, 2024 WL 5102709, at *5, rejected the identical argument that the CCPA "should control" because application of stricter privacy laws would "supplant . . . the detailed notice and 'opt out' framework of the CCPA," holding the "CCPA does not preempt" preexisting privacy rights. *Id*. TTD cites no authority to the contrary. TTD's reliance on the CCPA's "opt-out regime" as a shield is therefore misplaced; the CCPA and CPRA were designed to provide additional, non-exclusive tools for Californians to protect their privacy, not to create affirmatives defense for surveillance companies. Moreover, where, as here, Plaintiffs allege surreptitious surveillance, the opt-out regime is irrelevant because "if [Plaintiffs] did not know about the data collection, [they] could not have exercised" any right to opt out. *Deivaprakash v. Conde Nast Digital*, 2025 WL 2541952, at *3 (N.D. Cal. Sept. 4, 2025).[8]

The California Constitution is "the supreme law of our state," subject only to the supremacy of the United States Constitution. Cal. Const., art. III, § 1; *Sands v. Morongo Unified School Dis*t. 53 Cal.3d 863, 902 (1991). TTD's suggestion that the CCPA and CPRA "endorsed" or "expressly permits" conduct that otherwise violates the Constitution is incorrect as a matter of law; a statutory safe harbor exists only when a provision *actually bars the claim* or clearly permits the challenged

[8] Taken to its logical conclusion, TTD's nonsensical assertion—that by acknowledging the existence of privacy-invasive conduct in the CPRA, voters thereby relinquished any reasonable expectation of privacy with respect to that conduct—would mean that a plaintiff suing a peeping tom for spying on her no longer has any reasonable expectation of privacy because she has acknowledged the spying. The argument would also have the absurd consequence that virtually all case law finding a reasonable expectation of privacy in internet activity post-CCPA, including *Facebook Tracking*, was wrongly decided.

conduct, and courts may not imply a safe harbor from an overall regulatory scheme. *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal.4th 163, 182–83 (1999). The CCPA contains no clear permission for the persistent surveillance and profiling alleged here, and the CPRA's findings expressly condemn it. Plaintiffs have alleged a reasonable expectation of privacy.

2. Plaintiffs Have Alleged Highly Offensive Conduct

In the Ninth Circuit, determining whether conduct is "highly offensive to a reasonable person" is a holistic, fact-intensive inquiry that considers the likelihood of serious harm, the degree and setting of the intrusion, the intruder's motives, and whether countervailing interests or social norms render the intrusion inoffensive. *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). The "highly offensive" analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy, not on whether the conduct is common in the industry or regulated by statute.

As the Ninth Circuit has instructed, and courts within this District have repeatedly recognized, "[t]he ultimate question of whether [a defendant's] tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." *Id*. "Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is." *Lau v. Gen Digital Inc.*, 2023 WL 10553772, at *6 (N.D. Cal. Sept. 13, 2023) (quoting *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019)). "Only if the allegations 'show no reasonable expectation of privacy or an insubstantial impact on privacy interests' can the 'question of [a serious or highly offensive] invasion [] be adjudicated as a matter of law." *St. Aubin v. Carbon Health Techs., Inc.*, 2024 WL 4369675, at *12 (N.D. Cal. Oct. 1, 2024) (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 40 (1994)). Where, as here, defendants claim their data gathering practices are within "routine commercial behavior," dismissal is "particularly inappropriate . . . [because] Defendants are the only party privy to the true extent of the intrusion on Plaintiffs' privacy." *Hayden v. Retail Equation, Inc.*, 2022 WL 2254461, at *8 (C.D. Cal. May 4, 2022); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1061 (N.D. Cal. 2014) (rejecting "routine commercial behavior" defense because the "highly offensive . . . question is best left for a jury").

TTD's reliance on *In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014), *Gutierrez*, 2023 WL 8939221, at *4, and *Low*, 900 F. Supp. 2d at 1025, is misplaced, as these cases involved isolated or limited data collection—such as a single type of data or collection within a defendant's own platform.[9] None involved the comprehensive, persistent, aggregation of *both online and offline* data to create detailed, longitudinal dossiers on individuals, as Plaintiffs allege here. *See* CCAC ¶¶ 5–53, 115–45. The conduct here is far more analogous to the conduct found actionable in *Facebook Tracking*, *Katz-Lacabe*, and *Riganian*, where courts recognized that the surreptitious aggregation and commercialization of vast amounts of personal data—including sensitive and offline information and inferences—can be highly offensive to a reasonable person.[10] *See also* 105 Cal. Op. Att'y Gen. 26, 2022 WL 815641, at *5–8 (recognizing that "seemingly innocuous data points, when combined with other data points across masses of data, may be exploited to deduce startlingly personal characteristics," and describing the "mischief resulting from the creation and use of inferences by businesses," including political manipulation).

TTD's assertion that its commercial motive or the prevalence of its practices in the industry renders its conduct inoffensive is contrary to law.[11] TTD's factual assertion that its conduct benignly "helps keep the internet free" is both false and unsupported by any material in the CCAC, and is no basis to find a "countervailing interest" that undermines the invasiveness of TTD's

---

[9] *See also Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1126 (S.D. Cal. 2023) (disclosed data limited to a single website); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012); and *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) predate *Facebook Tracking* and are outdated, and have subsequently been found "unpersuasive" due to their "lack of consideration for California's privacy norms." *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1054 (N.D. Cal. 2018).

[10] *Hammerling* is readily distinguishable because it involved only the collection of limited app usage metrics in a manner arguably disclosed by Google. 615 F. Supp. 3d 1069. Nor did *Hammerling* hold that deception or breach of promise is required for a privacy claim; as *Facebook Tracking* and subsequent decisions confirm, the focus is on the nature and scope of the intrusion and whether it violates social norms, not merely on the presence of a misrepresentation.

[11] TTD misstates the holding of *Popa v. Microsoft Corp.*, 2025 WL 2448824, at *5 (9th Cir. Aug. 26, 2025). The court did not broadly hold that "'tracking . . . [online] interactions is a purely commercial, legal endeavor" (Mot. at 10); instead it found that collecting the plaintiffs' non-sensitive interactions with a single pet supply website that revealed simply *her pet food preferences* was not the sort of conduct traditionally actionable at common law. The allegations in *Popa* bear little resemblance to the allegations of extensive online and offline tracking and dossier-building here. Judge Bybee's concurrence in *Gutierrez v. Converse Inc.*, 2025 WL 1895315, at *3 (9th Cir. July 9, 2025)–opining that the "chat session" interception at issue there may be governed by the CCPA—helps Plaintiffs, as it demonstrates that, if true, the conduct was considered unacceptable under the CCPA framework.

conduct. To the contrary, the "highly offensive" inquiry is determined by whether the intrusion is unacceptable as a matter of public policy and social norms. *See Facebook Tracking*, 956 F.3d at 606; *Riganian*, 2025 WL 2021802, at *9 (rejecting argument that "commercially exploiting unlawfully obtained information is 'licit' merely because it is profitable."). Plaintiffs allege that TTD's practices have been widely condemned by privacy advocates and technology researchers, and that TTD's dragnet-style collection of their online and offline data and the resulting aggregation and sale constitutes precisely the sort of computerized "cradle-to-grave profiles" that the right to privacy under the California Constitution was created to constrain. CCAC ¶¶ 146–52, 188. Finally, as discussed above, nothing in the CCPA or CPRA remotely suggests that Californians approved of TTD's conduct; to the contrary, they explicitly *condemn* it. The weight of authority and the detailed factual allegations in the CCAC amply support the conclusion that TTD's conduct is highly offensive.

B. Plaintiffs Have Properly Pled ECPA and CIPA Claims

1. Trade Desk Intercepted Electronic Communications Content

Plaintiffs allege that through its tracking technologies, TTD intercepted full-string URLs, contents of search queries, including searches for and views of content on sensitive topics such as politics, mental health, and personal finance on 49 specifically identified websites (CCAC ¶¶ 6, 8, 9–11, 17, 30, 34, 43, 46, 229, 235), and actions taken on websites such as button clicks and purchases (*see, e.g., id.*, ¶¶ 95, 96, 100, 108–13). Plaintiffs further allege this information was captured "simultaneous" to the communication and "in transit" as it was being sent or received (*see, e.g.*, *id.*, ¶¶ 229, 235, 250), and that TTD used the information to generate detailed profiles and inferences about Plaintiffs' political views, health conditions, sexual preferences, and other personal characteristics (*see, e.g.*, *id.*, ¶¶ 122–23).

Notwithstanding these detailed allegations, TTD argues the allegations are insufficient to show interception of *contents* of communication. TTD's argument rests on an artificial distinction between "communications" and what it dismissively labels "actions," and incorrectly concludes the latter can never be protected under the ECPA. Mot. at 12. This is wrong: courts have repeatedly recognized that a wide range of digital interactions qualify as "content"—including full-string

URLs, search queries, "button" clicks, and even data such as vibration patterns. *See, e.g.*, *In re Google RTB Cons. Privacy Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) (URLs and related transmission data intercepted by companies like TTD in RTB are "contents" under the ECPA); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795 (N.D. Cal. 2022) (button clicks signaling a user logged into a healthcare account is "content," as are URLs that reveal sensitive medical conditions); *S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *7 (N.D. Cal. May 15, 2019) (vibration intensity data is "content" as it communicated the user's desired strength of touch); *Smith v. Rack Room Shoes, Inc.*, 2025 WL 1085169, at *4 (N.D. Cal. Apr. 4, 2025) ("URLs, button clicks, and viewing and cart history" constitute content); *Bland v. Roberts*, 730 F.3d 368, 386 (4th Cir. 2013) ("a user may use a single mouse click to produce [a substantive] message . . . instead of typing the same message with several keystrokes").[12] These holdings are consistent with the ECPA's broad definition of "contents" which includes "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8); *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051 (N.D. Cal. 2018) ("analysis for a violation of CIPA is the same as that under the federal Wiretap Act"); *see also In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015) (the "content" determination turns on how much substantive information the communication reveals).

TTD's reliance on *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014), and *Facebook Tracking*, 956 F.3d at 596, is misplaced. Both confirm that "a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication." *Zynga*, at 1108–09; *Facebook Tracking*, 956 F.3d at 605 (distinguishing *Zynga* and noting "content" sufficiently alleged via "a full-string detailed URL, which contains the name

[12] *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (C.D. Cal. 2021) both lacks any relevant analysis and is inconsistent with the substantial weight of authority in this District. *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1086 (N.D. Cal. 2018) found only that "simply opening a webpage or mobile application is not a communication with content," different conduct than that involved here. *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 70 (W.D. Pa. 2023) addressed a statute not at issue here, and also acknowledged that "'whether a URL involves 'contents' depends" "on how much information would be revealed by disclosure of the URL." *Id.* at 71.

of a website, folder, and sub-folders on the web-server, and the name of the precise file requested").[13] Plaintiffs here allege the interception of detailed URLs, including those that reveal searches and similar communications. *See, e.g.*, CACC ¶¶ 94–107, 113, 222.

TTD is also incorrect that Plaintiffs do not sufficiently allege the nature of the intercepted communications. *See* Mot. at 13. The CCAC alleges the topic of communications (e.g., politics, mental health, and personal finance) and identifies 49 specific websites from which these communications were intercepted. CCAC ¶¶ 6, 8, 9–12, 17, 19, 24, 30, 34, 37, 38, 43, 46, 53. Courts have rejected the notion that "Plaintiffs must plead the exact communications they had with" a given website to state a claim. *James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 956 (N.D. Cal. 2023); *see also In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 816 (N.D. Cal. 2020) ("[T]he Court rejects Defendants' suggestion that Plaintiffs must identify specific communications that Plaintiffs reasonably believed to be private and that were wrongly recorded."). And Plaintiffs' allegations here are far more specific than in TTD's cited cases. *See, e.g.*, *Jones v. Tonal Sys., Inc.*, 751 F. Supp. 3d 1025, 1038, 1043 (S.D. Cal 2024) (S.D. Cal 2024) (plaintiff only "allude[d] to the possibility" that highly sensitive or "private and deeply personal" communications could have been intercepted); *Hammerling*, 615 F. Supp. 3d at 1078, 1093 (alleging "usage and engagement" data from apps were intercepted, without identifying specific videos or documents viewed from within the apps); *Hughes v. Vivint, Inc*, 2024 WL 5179916, at *5 (C.D. Cal. July 12, 2024) ("Plaintiff does not clearly allege what personalized information of hers was actually collected").

2. Trade Desk Intercepted Communications "In Transit"

Under the ECPA, interception must occur contemporaneous to the underlying communication. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002). Under CIPA, it must occur while the communication "is in transit or passing over any wire, line or cable, or is being sent from, or received at any place within" California. Cal. Pen. Code § 631(a). Here, TTD argues its interceptions occur "*after* Plaintiffs visit those websites." Mot. at 14. But the CCAC states otherwise, alleging the interception occurs in "real time." CCAC ¶¶ 108–12 (explaining RTB), ¶ 229 ("simultaneous"), and ¶ 235 ("in transit" or while being sent or received). At the pleading

[13] TTD's reliance on *Hammerling* fails for the same reasons. 615 F. Supp. 3d at 1093 (recognizing "URLs that could reveal the particular articles users read would likely be more problematic").

stage, these allegations must be credited, making this a classic "question for summary judgment." *Hazel*, 2023 WL 3933073, at *4 (Breyer, J.) (denying dismissal where complaint alleged real-time interception); *Riganian*, 2025 WL 2021802, at *10 (timing "is a fact-intensive question that depends on how the challenged technology and process actually work"). For this reason, *Torres v. Prudential Financial*, is procedurally inapposite, having been decided on summary judgment. *See* 2025 WL 1135088 (N.D. Cal. Apr. 17, 2025).[14]

Torres is also factually distinguishable. In *Torres*, this Court found, *after discovery*, that CIPA was not satisfied because the communications at issue were "collected and stored as a series of *undeciphered* events." 2025 WL 1135088, at *5 (emphasis added). The Court took care to explain that *Facebook Tracking* instructed that contemporaneous interceptions of communications that are "used to create personal profiles that could be sold to advertisers" would satisfy the statute. *Id*. at *6. Here, Plaintiffs allege TTD's interceptions occur in *real time* for that precise purpose. *See, e.g.*, CCAC ¶ 1 (TTD "makes the data in these massive dossiers available for sale [and] use[s] that data to further surveil and manipulate"); *id.* ¶ 230. Indeed, Plaintiffs allege that the interceptions occur through TTD's "Real Time Conversion Events SDK," that TTD's own public documents describe as "Upload[ing] [i.e, intercepting] conversion events in *real-time*" (emphasis added). CCAC ¶ 104, n.45. Notably, in *Riganian,* the court found similar allegations sufficient at the pleading stage. *See* 2025 WL 2021802, at *10–11.

TTD's other cited cases do not support its position. *NovelPoster v. Javitch Canfield Grp*., supports Plaintiffs because it explains that the timing element is satisfied when "automatic routing software is used" to automatically send a duplicate of the communication during a "narrow window," as alleged here. 140 F. Supp. 3d 938, 951–52 (N.D. Cal. 2014); CACC ¶¶ 108–112, 229, ¶ 235. *Konop* is inapposite because it involved a communication that had been posted—and stored—on a message board for a lengthy period of time. 302 F.3d at 878. *Zynga* did not address timing. *Griffith v. TikTok*, was (like *Torres*) a summary judgment decision where plaintiffs did not submit *evidence* that the interception occurred while the communication remained, as Plaintiffs have alleged here. *See* 2024 WL 5279224, at *10 (C.D. Cal. Dec. 24, 2024). In any event, the

[14] *Torres* is in fact a later-decided order in *Hazel* (*sub nom.*, due to a change in named plaintiff).

precise technical details of TTD's conduct, including timing, are "a question for summary judgment." *Hazel*, 2023 WL 3933073, at *4.

3. The Consent Exception to the ECPA Does Not Apply

Regardless of any purported website consent,[15] TTD acted "for the purpose of committing any criminal or tortious act" under 18 U.S.C. § 2511(2)(d), which provides an exception to one-party consent. Contrary to TTD's suggestion, "the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception—its intended use—was criminal or tortious." *Rack Room Shoes*, 2025 WL 2210002, at *4. Plaintiffs allege that TTD intercepted their communications to inform "massive dossiers" that it makes "available for sale through various products and services to third parties, who subsequently use that data to further surveil and manipulate people." CCAC ¶¶ 1–4, 237–38. Such further use is sufficient to invoke the crime-tort exception. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (allegations that "Google intercepted [plaintiffs'] communications for the purpose of associating their data with preexisting user profiles" sufficient to invoke crime-tort exception); *Riganian*, 2025 WL 2021802, at *9 (same). Moreover, as many courts have recognized, TTD's "financial motivation is not a get-out-of-liability free card." *Stein v. Edward-Elmhurst Health*, 2025 WL 580556, at *6 (N.D. Ill. 2025) ("That's like saying that a bank robber's purpose was not to commit a crime—it was to make money"). As Judge Tigar recently noted in explicitly declining to follow *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001) and the courts that have followed it: "Put simply, committing a tort and seeking a profit are not mutually exclusive (if anything, the latter is often the reason for the former). . . . that conduct will not be excused on the grounds that [the defendant] acted in pursuit of profit." *Riganian*, 2025 WL 2021802, at *9; *see also R.S. v. Prime Healthcare Servs., Inc.*, 2025 WL 103488, at *7 (C.D. Cal. Jan. 13, 2025) ("a monetary purpose does not insulate a party from liability under the ECPA"); *Castillo v. Costco Wholesale Corp.*, 2024 WL 4785136, at *6 (W.D. Wash. Nov. 14, 2024) (same).

[15] TTD asserts that "the websites consented when they placed TTD's code on their websites." However, "consent is an affirmative defense for which [D]efendant bears the burden of proof." *Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024).

C. Plaintiffs Have Properly Pled a Pen Register Claim

Plaintiffs allege that TTD's pixels and Real Time Conversion Events SDK are "pen registers" under Cal. Pen. Code § 638.50(b) because they "record or decode" "addressing information," including IP addresses. *See, e.g.*, CCAC ¶¶ 219–35, 257–59; *see also Deivaprakash*, 2025 WL 2541952, at *1 (sustaining CIPA claim where third parties "collect the users' IP addresses"). TTD argues that Plaintiffs have not stated a CIPA § 638.51 claim because "an internet user's IP address is the equivalent of a caller's own phone number and therefore does not involve the recording of outgoing information, as the statute requires." Mot. at 16. Courts have repeatedly rejected this argument. CIPA defines a "pen register" as "a device or process that records or decodes . . . information *transmitted by* an instrument or facility *from which* a wire or electronic communication is transmitted." Cal. Pen. Code § 638.50(b) (emphasis added). "Nothing in th[at] statutory definition limits pen registers to those that operate the same way as a traditional phone pen register." *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 929 (N.D. Cal. 2024); *Garon v. Keleops*, 2025 WL 2522374, at *4 (N.D. Cal. Sept. 2, 2025) (collecting cases and holding same). Instead, "[b]y the plain meaning of § 638.50(b) . . . [a]ll that is required is that the Trackers record addressing information transmitted by the user's computer or smartphone . . . regardless of whether that addressing information pertains to the sender or the recipient of the communication at issue." *Shah,* 754 F. Supp. 3d at 929; *see also Mirmalek*, 2024 WL 5102709, at *4 (finding trackers were "pen registers" where they "'record' the addressing information by 'instruct[ing] the user's browser to send . . . the user's IP address'"); *Lesh v. Cable News Network, Inc.*, 767 F. Supp. 3d 33, 40 (S.D.N.Y. 2025) (same).[16]

TTD's professed confusion at the scope of Plaintiffs' pen register claim (Mot. at 16) is not well-taken: Plaintiffs unambiguously allege IP addresses are subject "routing, addressing, or signaling information," and also allege *in the alternative* that, to the extent the URLs and emails

[16] This Court already considered *Rodriguez v. Plivo Inc.*, 2024 WL 5184413 (Cal. Super. Oct. 2, 2024) in *Mirmalek* and found it unpersuasive. 2024 WL 5102709; *see* Case No. 24-cv-01797-CRB, Dkt. 26, *passim* (defendant unsuccessfully relying on *Plivo*). *Plivo* relied exclusively on legislative history rather than the statute's plain text. *Garon*, 2025 WL 2522374, at *5 (finding unpersuasive decisions that rely on "analysis of CIPA's legislative history" rather than "the plain statutory text"); *Riganian*, 2025 WL 2021802, at *12 (same).

intercepted by TTD's wiretapping technologies are determined by the Court not to be content, they are, by statutory definition, routing, addressing, or signaling information. CCAC ¶ 257. These alternative theories are consistent with Rule 8. Fed. R. Civ. P. 8(d). In any event, courts have found that software may be a "pen register" even if it collects the contents of a communication, so long as it also collects addressing information. *In re Meta Pixel Tax Filing Cases*, 2025 WL 2243615, at *5 (N.D. Cal. Aug. 6, 2025); *Gabrielli v. Haleon US Inc.*, 2025 WL 2494368, at *12 (N.D. Cal. Aug. 29, 2025).

Contrary to TTD's further argument that if its technology "had been the concern of California's pen register statute, then one would expect the legislature to have mentioned them somewhere in the statute's text or legislative history," (Mot. at 17) "the text of a law controls over purported legislative intentions unmoored from any statutory text," and "the Court may not replace the actual text with speculation as to Congress' intent." *Corner Post, Inc. v. Bd. of Governors of Fed. Rsrv. Sys.*, 603 U.S. 799, 815 (2024). And as to that text, "[i]f the drafters of Section 638.50 had intended for 'pen register' to be limited to telephone technologies, they knew how to do so—as evidenced by other sections of CIPA where they imposed such limitations." *Gabrielli v. Motorola Mobility LLC*, 2025 WL 1939957, at *11 (N.D. Cal. July 14, 2025).

Finally, TTD argues "[t]he consequences of adopting [Plaintiffs'] theory would be staggering," as "IP addresses and URLs are necessary to route data to the correct destination across the entire internet." Mot. at 16–17. This argument has likewise repeatedly been rejected, because "[t]o the extent that [Defendant] believes the statute may impose too many burdens when applied to the realities of modern technologies . . . the question of whether the statute's scope should be narrowed ultimately rests with the Legislature, not the courts." *Shah*, 754 F. Supp. 3d at 933. To be clear, TTD is not collecting IP addresses to simply "route data." Indeed, TTD is not even the website operator in this case. Instead, it is collecting this information to "compile[] digital dossiers, or profiles, on Class members," which are then used to target and manipulate them. CCAC ¶¶ 2, 156; *see also*, *e.g.*, *id.* ¶¶ 4, 9, 19, 32, 42, 46, 65, 188. That conduct is not "necessary to operate or maintain" a website. *Rodriguez v. Autotrader.com*, 762 F. Supp. 3d 921, 930 (C.D. Cal. 2025); *Motorola Mobility*, 2025 WL 1939957, at *12.

D. Plaintiffs Have Properly Pled CDAFA Violations

CDAFA is a comprehensive statutory scheme preventing "tampering, interference, damage, and unauthorized access" to "computer data and computer systems." Cal. Penal Code § 502(a). TTD's alleged conduct clearly violates this statute.

Plaintiffs Have CDAFA Standing. Courts have repeatedly recognized that when a defendant "unjust[ly] profits" from Plaintiffs—as alleged here (CCAC ¶¶ 125, 138, 278)—this constitutes "damage or loss" under CDAFA. *See Rack Room Shoes*, 2025 WL 2210002, at *3 (disgorgement theory satisfies CDAFA standing); *Rodriguez*, 772 F. Supp. 3d at 1110 (finding CDAFA standing where "Google profited from the misappropriation of their data"). Plaintiffs also allege that TTD's technology causes "disguise[d]" first-party cookies and other identifiers (*e.g.*, UID2 tokens) to self-propagate in Plaintiffs' local storage, using device resources without permission. CCAC ¶¶ 275, 280. This also suffices for CDAFA standing. *See Williams v. Facebook, Inc.*, 498 F. Supp. 3d 1189, 1200 (N.D. Cal. 2019) ("depletion of device resources" establishes CDAFA standing); *Rodriguez*, 772 F. Supp. 3d at 1110 ("even small harms" like "depletion" of "bandwidth" establish CDAFA standing); *In re Meta Healthcare Pixel Litig.*, 713 F. Supp. 3d 650, 656 (N.D. Cal. 2024) (use of storage, computer resources, and unjust profit confer standing). Ignoring these robust allegations, TTD focuses on cases alleging *additional* theories of CDAFA standing, *i.e.*, that the defendant's conduct caused privacy harms or diminished the value of their data.[17] *See* Mot. at 17–18. While Plaintiffs maintain that these are also viable theories of CDAFA standing (*Williams*, 498 F. Supp. 3d at 1200 (accepting a diminution in value theory in light of *In re Facebook Priv. Litig.*, 572 F. App'x 494 (9th Cir. 2014)), that TTD has not challenged Plaintiffs' other bases for standing is dispositive.

Plaintiffs Satisfy Rule 8 and Rule 9(b). TTD's claim that it lacks "fair notice" of the "factual basis" for Plaintiffs' CDAFA claims is equally meritless. Mot. at 18. Even if Rule 9(b)

[17] Only one case cited by TTD—*Shah v. Cap. One Fin. Corp.*, 768 F. Supp. 3d 1033, 1048 (N.D. Cal. 2025)—found that unjust "profit[s]" cannot confer CDAFA standing absent a corresponding "loss", but that decision is inconsistent with controlling precedent. *See Facebook Tracking*, 956 F.3d at 600 (disgorgement of profits under California law does not require a "corresponding loss").

applies—which Plaintiffs dispute[18]—that standard is satisfied because Plaintiffs allege the "who" (TTD) "what" (subverted privacy protections and the ordinary operation of their devices and services) "when" (at the time Plaintiffs and Class Members visited web properties) "where or how" (through its technology embedded on web properties, which propagates UID2 and other identifiers in local storage, and intercepts their data to build user profiles). *See* CCAC ¶ 275. TTD's suggestion that Plaintiffs somehow violated the pleading standard because they bring CDAFA claims based on its use, access, and disruption of computer *systems* (defined to include "devices" that contain "computer programs") as well as computer *services* (defined as "computer time, data processing, [and] storage functions") makes little sense. Mot. at 18 n.9. That TTD violated CDAFA in multiple ways is a reflection of how invasive its conduct is—not a pleading deficiency.

Plaintiffs Allege TTD Acted "Without Permission." This requirement is satisfied so long as a defendant acts without consent. *See Brown*, 685 F. Supp. 3d at 940 n.38; *see also Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016). Plaintiffs adequately allege there was no consent, so this requirement is satisfied. CCAC ¶¶ 276, 280. As multiple courts have recognized, TTD's suggestion that "without permission" requires showing a circumvention of code-based barriers (Mot. at 19) "is belied by [*United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015)], in which the Ninth Circuit . . . rejected the idea that, under the CDAFA, technical circumvention was necessary." *Brown*, 685 F. Supp. 3d at 940 n.38; *see also Cherkin v. PowerSchool Holdings, Inc.*, 2025 WL 844378, at *6 (N.D. Cal. Mar. 17, 2025). But even if this were required, Plaintiffs allege that TTD secretly assigns a UID2 and "disguise[s]" its third-party cookies as first-party cookies to circumvent code-based privacy protections designed to prevent this type of third-party tracking. *See* CCAC ¶ 152, 280; *see also Greenley v. Kocahva, Inc.*, 684 F. Supp. 3d 1024, 1049 (S.D. Cal. 2023) (allegations that defendant's technology is an "end-run" around built-in "privacy framework" satisfy "technical or code-based barriers" requirement); *Brown*, 525 F. Supp. 3d at 1075 (allegations that code was "hidden" itself satisfies "technical or code based" barrier requirement). Neither *Perkins* or *Guitierrez*, on which TTD relies, contained

[18] *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 455 (N.D. Cal. 2018), *on reconsideration in part*, 386 F. Supp. 3d 1155 (N.D. Cal. 2019) (noting Rule 9(b) applies to CLRA, UCL, and FAL but making no such acknowledgment in sustaining CDAFA claims).

similar allegations. *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014) (no allegation of "what" barriers were in place or "who" and "how" they were overcome); *Gutierrez*, 2023 WL 8939221, at *4 (only alleging "without permission" in the "ordinary sense").

Plaintiffs Allege Claims Under 502(c)(1) and (c)(4). Plaintiffs plausibly allege CDAFA(c)(1) and (4) claims because TTD's technology places cookies and other identifiers in their local storage and redirects their private data to its servers for its own use. *See* CCAC ¶ 275(a). *see also In re Meta Healthcare Pixel Litig.*, 713 F. Supp. 3d at 656 (allegations that tracking technology places "cookies[]" on their "devices" and "redirect[s]" data to defendant's own servers sufficient to allege defendant "altered" their "data or devices"); *Zarif v. Hwareh.com, Inc.*, 2025 WL 486317, at *13 (S.D. Cal. Feb. 13, 2025) (sustaining CDAFA claims where tracking technology "interfaced with [plaintiffs computer] and "made use of [her] data"). TTD's reliance on *McGowan v. Weinstein*, 505 F. Supp. 3d 1000, 1020 (C.D. Cal. 2020) in arguing that its "use" of data is not the type of harm envisioned by CDAFA (c)(1) and (4) is a red herring. Mot. at 19. That case involved the "use" of a "digital copy" of an "unpublished manuscript" to protect the public reputation of Harvey Weinstein. *Id.* The court found this "categorically distinct" from the purpose of CDAFA. *Id.* The opposite is true here where the use of data stems directly from TTD's access and use of Plaintiffs' local storage to place unauthorized cookies and identifiers, both of which fall within CDAFA (c)(1) and (4)'s purview.

Plaintiffs Allege Computer Contaminants Under 502(c)(8). TTD's own authority acknowledges that a "computer contaminant" includes any "computer instructions" that "consume computer resources, modify, destroy, record, or transmit data" or otherwise "usurp . . . normal [computer] operation[s]." *See In re iPhone Application Litig.*, 2011 WL 4403963, at *13 (N.D. Cal. Sept. 20, 2011) (citing CDAFA 502(c)(8)). There is no question that TTD's technology falls within this definition of "computer contaminant." *See In re Meta Healthcare Pixel Litig.*, 713 F. Supp. 3d at 657 (finding pixel technology that "log[s]" and "track[s]" actions qualifies as a "contaminant"). TTD's assertion that finding it liable would be akin to "criminaliz[ing] the internet" is both false and not a basis to disregard the law. *See Brown*, 685 F. Supp. at 940 (rejecting argument that holding Google liable "would in effect criminalize routine internet functionality"). Its final arguments—

that it does not "'introduce' anything" and merely "receives" data from third parties (Mot. at 20)—are purely factual challenges that are inappropriate at this stage. *Brown*, 685 F. Supp. 3d at 940 (rejecting similar argument on summary judgment as a "triable issue" for a jury).

E. The Rule of Lenity Does Not Bar Plaintiffs' Statutory Claims

"[T]he rule of lenity applies if, after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute." *Joffe v. Google, Inc.*, 746 F.3d 920, 935–36 (9th Cir. 2013). TTD identifies no such grievous ambiguity or uncertainty in the ECPA, CIPA, or CDAFA. As to the ECPA, "it has been repeatedly recognized that the ECPA applies to electronic communications transmitted via the internet." *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 157 F. Supp. 2d 286, 290 (S.D.N.Y. 2001) (collecting cases). This is evident from the plain text of the statute, which broadly defines an "electronic communication" as "*any* transfer of signs, signals, writing, images, sound, data, or intelligence of any nature[.]" 18 U.S.C. § 2510(12) (emphasis added). Thus, courts have consistently sustained ECPA claims like those here based on information collected from internet communications. *See, e.g.*, *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 796; *Brown*, 685 F. Supp. 3d at 935-36.

The California Supreme Court and federal district courts have universally rejected rule of lenity arguments involving the CIPA; indeed, this Court rejected this same argument only last week. *Fregosa*, 2025 WL 2886399, at *9; *see also Smith v. LoanMe*, 11 Cal. 5th 183, 202 (2021) (rejecting application of rule of lenity to CIPA § 632.7); *Riganian*, 2025 WL 2021802, at *12 (LiveRamp "has not established any 'grievous ambiguity' in the statute's express language."); *Garon*, 2025 WL 2522374, at *6 (same); *Deivaprakash*, 2025 WL 2541952, at *5. Courts have also rejected the rule of lenity's application to the CDAFA for the same reason. *Brown*, 685 F. Supp. 3d at 940. TTD cites no case applying the rule of lenity to the statutes at issues here.[19]

F. Plaintiffs Have Properly Pled Unjust Enrichment

TTD's four single-sentence arguments for dismissing Plaintiffs' unjust enrichment claim are foreclosed by recent, directly on-point authority from this District. ***First***, California courts have

[19] *Vita v. New England Baptist Hosp*, 243 N.E.3d 1185, 1188–95, 1204 (Mass. 2024); *Gray v. Twitter Inc.*, 2021 WL 11086642, at *8–9 (W.D. Wash. Mar. 17, 2021); and *U.S. v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) are all inapposite as they address statutes or terms not at issue here.

repeatedly held unjust enrichment is cognizable as a quasi-contract or restitution claim, regardless of label. *Riganian*, 2025 WL 2021802, at *13 (allowing claim for unjust enrichment in identical circumstances); *Pro. Tax Appeal v. Kennedy-Wilson Holdings, Inc.*, 29 Cal. App. 5th 230, 238 (2018) ("The elements of a cause of action for unjust enrichment are simply stated as receipt of a benefit and unjust retention of the benefit at the expense of another."). ***Second***, courts have held that a claim lies where a defendant unjustly profits from the violation of legally protected privacy rights, even absent out-of-pocket loss or traditional quasi-contractual circumstances. *Riganian*, 2025 WL 2021802, at *13 (relevant inquiry is whether "retention of the benefit would be unjust—not on identifying 'mistake, fraud, coercion, or request' as the only possible ways in which such retention could be unjust"); *Katz-Lacabe*, 2023 WL 6466195, at *6 ("Oracle's collection of data from third-party websites . . . conferred a benefit upon Oracle at the expense of the privacy of their data."); ***Third***, California law imposes no privity requirement and benefits may be indirect. *Id*. at *7; *In re Gen. Motors LLC CP4 Fuel Pump Litig*., 393 F. Supp. 3d 871, 882 (N.D. Cal. 2019). ***Finally***, TTD's argument that Plaintiffs have not pled the inadequacy of legal remedies under *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834 (9th Cir. 2020), is both premature and contrary to the prevailing authority in this District. As courts have explained, "*Sonner* does not preclude a plaintiff from pleading equitable remedies in the alternative," and "*Sonner* has limited applicability to the pleading stage because it pertained to circumstances in which a plaintiff dropped all damages claims on the eve of trial." *Katz-Lacabe*, 668 F. Supp. 3d at 949. Plaintiffs' request for injunctive relief also makes *Sonner* inapplicable. *Hass v. Travelex Ins. Servs. Inc.*, 555 F. Supp. 3d 970, 976 (C.D. Cal, 2021). TTD's *Sonner*-based challenge should be rejected. *See Veritas Techs. LLC v. Cushman & Wakefield, Inc.*, 2022 WL 222527, at *11 (Breyer, J.) (N.D. Cal. Jan. 25, 2022) (rejecting *Sonner* unjust enrichment argument).

V. CONCLUSION

Plaintiffs respectfully submit that the Court should deny TTD's motion in its entirety,[20] but that any dismissal, in whole or in part, should be without prejudice and with leave to amend.

[20] Because TTD's other arguments fail, Plaintiffs' declaratory relief claim should stand. *See Hammerling*, 615 F. Supp. 3d at 1097 (dismissing declaratory relief claim only where underlying claims were also dismissed).

Dated: October 17, 2025

Respectfully submitted,

/s/ *Michael W. Sobol*
Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice*)
lpittman@lchb.com
Danna Elmasry (*pro hac vice*)
delmasry@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

/s/ *Jay Barnes*
Jason 'Jay' Barnes (*pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (*pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (*pro hac vice*)
atruong@simmonsfirm.com
Sona Shah (*pro hac vice*)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel: 212-784-6400
Fax: 212-213-5949

/s/ *Christian Levis*
Christian Levis (*pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (*pro hac vice*)
afiorilla@lowey.com
Rachel Kesten (*pro hac vice*)
rkesten@lowey.com
Yuanchen Lu (*pro hac vice*)
ylu@lowey.com
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035

/s/ *Philip L. Fraietta*
Philip L. Fraietta (SBN 354768)
pfraietta@bursor.com
Max S. Roberts (*pro hac vice*)
mroberts@bursor.com
Victoria X. Zhou (*pro hac vice*)
vzhou@bursor.com
Joshua R. Wilner (SBN 353949)
jwilner@bursor.com
BURSOR & FISHER, P.A.
50 Main Street, Suite 475
White Plains, NY 10606
Telephone: 914.874.0710
Facsimile: 914.206.3656

Attorneys for Plaintiffs and the Proposed Classes

ATTESTATION

Pursuant to Civil Local Rule 5.1 regarding signatures, I attest that concurrence in the filing of this document has been obtained from the other signatories.

Dated: October 17, 2025

/s/*Michael W. Sobol*
Michael W. Sobol
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP